VOCAB

Field Programmable Gate Array (FPGA) is a reconfigurable integrated circuit that can be programmed after manufacturing. It allows for parallel processing, customization, and high performance, making it ideal for tasks like digital signal processing and hardware acceleration in telecommunications, automotive, aerospace, and electronics.

Attestation is when you verify the confidentiality and integrity of data or a message.

Intermediate Distribution Frame (IDF) is a cable rack used to manage and connect telecommunications and network wiring between an organization's Main Distribution Frame (MDF) and end-user devices. IDFs help organize and distribute network cables, improving network efficiency and management in larger buildings or campus environments.

Infrastructure as code(IaC) describes an infrastructure as servers, networks and apps as code. The code can then be duplicated and built out on different instances on different clouds.

BGP(border gateway protocol) Sets the framework for how certain information should be routed across the internet

NGFW(next generation firewall) An application layer(7) firewall. Has many built in functions like a DNS filter and an IPS

FRR(False rejection rate) A measure of the likelihood that a biometric security system will incorrectly reject an access attempt by an authorized user

Contingency vs business continuity

CVSS(common vulnerability standard scoring)

DMARC(Domain message authentication reporting and conformance) used to authenticate emails and deal with any emails it determines junk through its configuration

OSINT(Open source Intelligence)

GPG(GNU privacy guard) - Open source public key (asymmetric) cryptography standard

Elliptic curve cryptography(ECC) is a type of public key cryptography, so each user has a pair of ECC keys: a public key and a private key. The public key is shared with others. Then anyone can use it to send the owner an encrypted message. The private key is kept secret – only the owner knows it.

BPDU(Bridge protocol data unit)

OSPF(Open shortest path first)

GCM (Galois/Counter Mode) is a block cipher mode that provides both encryption and authentication, ensuring data confidentiality and integrity. It is fast, parallelizable, and widely used in protocols like TLS and IPsec. GCM requires a unique nonce for each encryption to maintain security.

Message digest - out of date hash algorithm

DNAT(Destination network address translation) The destination IP packet is modified once hitting a private network and then will translate the destination to a specific point within the private network.(someone on the internet trying to access a corporate web server.)

ESP(Encapsulated security payload)

GRP(Generic routing encapsulation) Used to create tunnels in VPNs.

TCP is a connection-based protocol and **UDP** is connectionless.

Routing is the process of selecting paths in a network along which to send data packets. Routers, which are network devices, determine the optimal path for data transmission based on factors like distance, congestion, and network topology. Routing ensures efficient, reliable data delivery between source and destination across interconnected networks, such as the internet.

Shimming/Shim is the process of changing the external behavior of an application while making no changes to the application's code. What is the definition of shimming in cybersecurity? Shimming is a cyberattack technique that allows a malicious code to be inserted into a legitimate process or application

OPAL(open vulnerability assessment language)

ARP(address resolution protocol)

CBC(cipher block channeling)

AIS(automated indicator sharing)

CSU(Channel service unit) - used in converting telephone calls into transmissible packets to send to the callers LAN.

ASLR(Address space layout randomization) - used in preventing buffer overflow attacks, randomly arranges data storage spaces in the memory.

DHE (diffie-hellman ephemeral)

NTFS(new technology file system)

HMAC(Hash message Authentication Code)

Zero trust control plane(use treppa technologies video)-

MTU(maximum transmission unit)

RC4 was used in legacy systems like WEP

Counter mode(CTM)A block cipher mode that combines a unique counter with encryption key to generate a stream of pseudorandom data blocks which are then used for encrypting data

ECB (Electronic Codebook) is a mode of operation for block ciphers. In ECB mode, each plaintext block is encrypted independently using the same key. This means that identical plaintext blocks will always produce identical ciphertext blocks when encrypted with the same key. While ECB is simple and straightforward, it has significant security weaknesses

FTPS vs SFTP - FTPS is secure file transfer and SFTP is file transfer over ssh.

SRTP (Secure Real-time Transport Protocol) is a security protocol designed to provide encryption, message authentication, and integrity for real-time voice and video communication over IP networks.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) is an encryption protocol used in wireless networks, specifically within the **WPA2 (Wi-Fi Protected Access 2)** standard. CCMP enhances security by providing both data confidentiality and integrity. It uses the AES (Advanced Encryption Standard) algorithm in counter mode for encryption, combined with the Cipher Block Chaining Message Authentication Code (CBC-MAC) for ensuring data integrity and authentication. CCMP is designed to replace TKIP and provides stronger security measures for protecting Wi-Fi communications.

RSA (Rivest-Shamir-Adleman) is a widely-used public key cryptographic algorithm named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman. It is used for secure data transmission and is based on the mathematical difficulty of factoring the product of two large prime numbers. RSA involves two keys: a public key, which can be shared with everyone, and a private key, which is kept secret. Used in verifying digital signatures.

Perfect Forward Secrecy (PFS) is a security feature used in cryptographic protocols to ensure that session keys are not compromised even if the server's long-term private key is compromised. PFS achieves this by generating unique session keys for each communication session, which are not derived from the server's private key.

DHE (Diffie-Hellman Ephemeral) is a key exchange protocol that generates temporary keys for each session, ensuring that each session has its own unique key. This provides forward secrecy, meaning that even if one session's key is compromised, past and future communications remain secure.

TKIP (Temporal Key Integrity Protocol) is a security protocol used in Wi-Fi networks to enhance **WEP** encryption. Introduced in the IEEE 802.11i standard, it dynamically generates unique encryption keys for each data packet, improving security. TKIP was widely used with WPA but has been largely replaced by more secure protocols like WPA2 and WPA3.

IPSec(internet protocol security) contains the following elements: **Encapsulating Security Payload (ESP)**: Provides confidentiality, authentication, and integrity. **Authentication Header (AH)**: Provides authentication and integrity. **Internet Key Exchange (IKE)**: Provides key management and Security Association management.

TGT: Ticket Granting Ticket - A ticket used in the Kerberos authentication protocol that allows a client to obtain additional tickets for accessing other services without needing to be re-authenticated.

TACACS+ — encrypts the entire payload of the packets (except the header), and supports various authentication mechanisms, such as PAP, CHAP, and MS-CHAP. In summary, TACACS is a network protocol that enables centralized AAA services for network devices.

Parts of the zero trust- control plane and data plane

S/MIME (Secure/Multipurpose internet Mail Extensions) is a widely accepted protocol for sending digitally signed and encrypted messages. S/MIME in Exchange

Online provides the following services for email messages: Encryption: Protects the content of email messages.

Internet key exchange (IKE) is a protocol that establishes a secure connection between two devices on the internet.

New Technology LAN manager(NTLM) was a windows authentication protocol that was replaced by Kerberos

IRC(Internet relay chat) provides **real time** Internet chat.

XML(Extended markup language) is a coding language like HTML but for creating a text based solution for organizing and structuring data securely.

GPO(group policy object) is a windows solution for managing users and policies over a network.

PGP(pretty good privacy) is an open source asymmetric encryption algorithm used in the Digital Signature and Certificate infrastructure

GPG(GNU privacy guard) is an asymmetric encryption algorithm used in the public key infastruce as well as the PGP, very similar.

IaaS: Allows for an entire cloud network infrastructure
SaaS: Prebuilt ready to use software
PaaS: Gives all the framework to host and configure your own self developed software or apps.

DHCP -A protocol that contains all configurations for a host IP connecting to its subdomains. This includes subnet masking.

UEFI replace the **Master Boot record** as a set of code delivered upon start up of a system

L2TP - replaced PPTP as the VPN connection protocol. Uses UDP. Needs IPSec for encryption.

TSIGS are used to secure and authenticate DNS server communication during zone transfer and other digital transactions.

LINKS

Acronyms:https://quizlet.com/850633004/learn
Basic terms:https://quizlet.com/868319633/security-sy701-flash-cards/?exitTest=1
Practice tests:https://www.examcompass.com
Messer vids:https://www.youtube.com/playlist?list=PLG49S3nxzAnl4QDVqK-hOnoqcSKEIDDuv
Acronyms pt2: https://quizlet.com/845696207/flashcards
Sunny Classroom YT:https://www.youtube.com/@sunnyclassroom24

TOPICS TO REVIEW

COPE, CYOD, BYOD
TPM
SCAP vs SOAR
Authentication headers
SaaS, PaaS, Maas, IaaS,
Leap, Eap

NOTES

1.0

1.2 Zero Trust-

Adaptive identity- considers the source of the ask/request, and what would come with giving this person access.(risk indicators would be like relationship,location,connections,etc)

Threat scope reduction- eliminate as much access as possible

security zones- where are they connecting from and where are they connecting too.(implicit trust allows someone from the trusted zone like possibly someone at a headquarters automatically is allowed into the next trusted or internal zone)

PEP- where decisions are made on whether one is to be allowed or denied(many devices and systems checking allowance) just collects all the data about the requester.

Policy decision point- the process of using the data the policy enforcement point gathers and sends it to the **POLICY ENGINE** where it then makes an evaluation whether to grant, deny or revoke.

Policy administrator communicates with the PEP to allow the decisions to be made and what and what's not acceptable to trust. Bases decision off of policy engine.

Deception and disruption-

honeypots- attracts attackers and allows you to monitor them to see what is being used to attack and why. General term.

Honeynet- a real network that simulates a real network, consisting of honeypots. Could be servers, workstations, routers and firewalls.

Honeyfiles- seemingly important, just fake data file

Honeytokens- data that is inside a honefile to allow us to track when and where certain fake information was used.(fake password or API token)

1.3 Change management

Change is one of the most common risks in enterprise, that's why there needs to be a formal process and environment to make sure change is needed and how to make sure it works.

Starts with the owners wanting a change

Stakeholders are people that are impacted by a change.

Impact analysis- high medium or low risk(risk severity). What will happen if we don't make a change and what could happen if we do.

Sandbox- testing environment

Technical change management

No such thing as simple upgrade
The scope may need to be expanded but that does not give you permission to change everything you want.
A well documented process is very important to limit dysfunction and down time.

Downtime should be as automated as possible

Daemon is a process that runs in the background without user interaction

Legacy systems can sometimes have conflicts with new changes.

Dependencies can require other dependencies to upgrade the intended upgrade.

1,4 Public key infrastructure

Policies, procedures, hardware, software, and people who deal with Digital Certificates.

VERY BIG ENDEAVOR

Symmetric encryption uses 1 key and to encrypt and decrypt a shared key. Like passing a briefcase from one person to another. Referred to as a secret key algorithm or a Shared Secret. Hard to use above 10 individuals/devices. (AES,TwoFish, RC4-6,IDEA,Salsa)

Asymmetric encryption - Public and private keys (two or more mathematically related keys.) used to send you data with the public key and you use the private key to decrypt the data. RSA, PGP & GPG are Asymmetric. If someone has your public key they can only send the data, as you would need the private key in order to decrypt it.

Key escrow holds your private key and can be used to decrypt your data, can be legitimate and sometimes even necessary to keep up with tons of data.

Encryption

Encrypting data at rest(stored data) is an essential part of providing confidentiality.
Anything on an SSD,HDD, USB, etc is data at rest.

Full disk/partition encryption types like BItlocker or FileVault. They encrypt your full drive.

A **bec attack** is a form of phishing that relies on gaining confidential information.

File encryption is like **EFS(Encrypted file system)** which is the windows version of it. There are other third party apps that do the same thing. Just files, not entire drives.

Transparent encryption- is when you encrypt an entire database
Record Level encryption is when you encrypt only data columns in a database(like SQL btw). More complex
Uses a symmetric key for both

VPN crates and encrypted tunnel to allow them on to a network.most of the time client based and uses SSL/TLS

IPSec creates secure tunneling from one worksite to another remote worksite.

DES(DATA ENCRYPTION STANDARD)- breaks up 64 bbit plaintext into different plaintexts and turn them into 16 round each which then turns them into their final stage which becomes the 64 bit cipher text

AES(ADVANCED ENCRYPTION STANDARD)- Takes the plaintext and a secret key, using the standard (128, 192, 256 Bits) it then converts the two together into a cipher which then becomes the ciphertext in the corresponding bit count.

In keys, a symmetric key is common to be 128 bits or more. A brute force attack is common with evolving processors. Asymmetric is far more complex and uses tons of math and prime numbers to develop a key pair of 3,072 bits or larger.

Key Stretching is when you re-encrypt a message or data to enforce security. Discourages Brute Force attackers.

KEY EXCHANGE

Out of band is when you transfer a key out of the network. Like telephones or handing over stuff.
In-band key exchange sends data across the network. This is needed in networks as time is of the essence.

Session key is when a server uses asymmetric encryption to allow a secure symmetric connection called a session.the server receives data from a client using a randomly generated symmetric key that then uses its own private key to decrypt as it created the encrypted symmetric key. Temporary.

Symmetric key from asymmetric example: Bob has a private key and Alice's public key. Alice has her private key and Bob's public key. Since they each know their own private keys and public keys, along with each other's public keys they are able to encrypt data only between them. As the private keys can decrypt their own public key's data. They both build the same symmetric key and therefore can connect.

Encryption technologies

TPM(Trusted Platform Module) Hardware that encrypts and creates keys. Cryptographic processor.
HSM(Hardware Security Module)Large environment storage for encryption keys. Holds 1000s of keys for servers.

Key management system is usually a GUI that centralizes keys in an area separate from data. Allows for logging and reporting.
Secure enclave a protected area for data. Allows it to remain private no matter who gets access to your devices. Performs AES inside hardware. A central security processor separate from the regular CPU.

OBFUSCATION

Process of making things unclear can be reverse engineered if you know the method it was hidden.
Steganographgy is concealing data inside pictures.
Method of security through insecurity.

Common types of steganography
-Network based, embed in messages in TCP packets
-Use an image and imbed it in the file
-Invisible watermarks that only be seen under certain conditions

Tokenization is replacing sensitive data with random data that can only be decrypted after it has reached the person with the cipher to decrypt. Think of how stores send your card information to the bank and broker departments.

NFC(near field communication)- apple pay

HASHING AND DIGITAL SIGNATURES

Integrity
Impossible to recover initial message its a one way trip
Digital signatures are used for authentication, integrity, and non repudiation.

SHA256 is the most common hashing algorithm
A **hash function** is supposed to be taking an input and creating a fixed string.

Collision is when you take two different inputs and they have the same hash.
.
MD(message digest) and **Checksums** are all hash.
MD5 hash has collision issues, don't use it.

Verifies that files you intend to download(like the file on the website) match the files you actually download
Instead of storing passwords with encryption we store them as a salted hash. This helps us make sure no one can crack it but also it can be retrieved. Salts make it so even if every single user uses the same password we see different hashes for each.

Rainbow Table-reverse engineers hashes. Rainbow tables don't work with salted hashes as they work based off of the common algorithms for hashing each possible input. If the salts are random it throws off the whole attack. Would require brute forcing instead which takes much much longer.

Digital signatures prove the message wasn't changed, proves the source, and shows it is not fake. Verifies it with the public key for that user because it is signed with the sender's private key. This is asymmetric.

ECDSA(Elliptical curve digital signature algorithm) is used for smaller IOT devices. ECC keys are far smaller than that of a public key hashing algorithm like SHA.

BLOCKCHAIN TECHNOLOGY

A distributed ledger that keeps track of individual transactions.
Everyone has a ledger and everyone can keep a copy of it.
USED IN:
-Payment processing
-digital ID
-digital voting
-etc

An NFT keeps track of itself on the blockchain.Each user has a record of its transaction data.

It can be used to detect fake transactions.

CERTIFICATES

Public Key Certificate binds a public key with a digital signature so you always know who you are connecting with if they have a public key.

CA(Certificate Authority) Who trust the person signs their certificate therefore as long as we trust the CA we can trust them.

PKI(Public Key Infrastructure) See earlier

Web of trust allows us to trust people that mutual people we know trust.

Windows and other third parties have certificate authority software and services.

X.509 is the standard format for digital certificates.

Root of trust- uses a third party like Security enclave, HSM, or CA to decide on trust.

Third part certificate- bought from a third party CA.*(like azure or aws)

CSR - Certificate Signing Request uses our information to create one which is sent to the CA and validates you based upon the root of trust and your information and reasons. They will validate it and send it back to you.

Windows CA and OpenCA all have their own private certificate authority systems which can be used on private networks to verify signatures.

Self Signed certificate - are for internal networks, not to be used on the web.

SAN(Subject alternative name)-. Uses any device with a subject alternate name or an alternate DNS name. (for example if it was Google.com and Google.org)

Wildcard- allow for multiple subdomains und

er a single domain name(like docs.google or slides.google)

CRL(Cert revocation list) is managed by a **CA** and shows who has been revoked.

OCSP(online certificate status protocol) Stapling can be used to allow us to post our cert status during the handshake of the server. The CA uses a digital signature to verify the Status is correct. New age method of authenticating certificates.

2.0

2.1 THREAT ACTORS

internal /external
Wealth is a factor in determining attackers and their method.
Look at attackers' skill levels.
Nation states- government security operations, could be used in war. Commonly advanced persistent threat.(APTs)
Script Kiddies use basic methods commonly libraries and scripts. Motivated by the hunt not financial gain. Looks for easy ways in
Hacktivist- has philosophical or ethical concerns for why they hack you.
Organized crimes are in the business of making money.
Shadow IT- Insider who works around the rules that the IT department makes. Makes their own network or applications that are not a part of the total system.

2.2 THREAT VECTOR

AKA Attack vectors.

Message based vectors(social engineering) are a common attack. Usually phishing

Unsecured network vectors:
-Outdated wireless like WEP,WPA, or WPA2
-insecure interfaces
-rogue access points(look over scans to see these)
-bluetooth(bluesnarfing is stealing data over bluetooth bluejacking is sending data over bluetooth.)

802.1x Prevents a lot of these by stopping anyone without proper credentials.

Open service ports allow attacks. It is important to limit access from these and to make sure any software used is updated to prevent entrance from misuse or exploitation from said software. Firewalls can limit ports.

Default credentials are a threat/attack vector.

Supply chain vectors ride alongside the hardware you are installing. They come with the technology you buy and usually neither party knows about it. MSP's (managed service providers) have been a target for these attacks(target credit card leak)

Typosquatting is when they use a similar website url to get you to click on it]

Pretexting gives you a fake story in order to get you to follow along.

Watering hole waits for you to use a service or third party sites and uses them against you. They will attack a smaller or weaker third party and then use that to get themselves into your network. They could even poison the hole for everyone who enters the site but they are usually pursuing a specific target.

Memory injections are when malware works in the memory. It can inject itself into other functions. Adds code into an existing process and now the malware can function and root through the memory to achieve a goal. DLL is the most common memory injection. They inject a link by putting the address of a link inside of a traditional process that would call for a common address for its intended function.

Buffer overflow is when memory is overwritten and overflows into another form or function. Attackers go through entire apps trying to overflow each data path. If they find one that overflows that is always repeatable and gives them a function they use it to achieve their goals. (Overflows bytes into the columns adjacent to it example image)

RACE CONDITIONS is when two events happen at the same time and it has an unexpected outcome. **TOCTOU(time of check to time of use)** can be an example when you don't know if the attacker is still inside the system.

XSS is when vulnerabilities come from your browser. Commonly use Java Script, since it is commonly trusted. Example: a hacker sends a malicious link that allows the target to open up a link to a legitimate site but with the code injected in it. That code will send data like cookies or session ID's to the attacker. Can use inputs on websites to embed scripts into a website(**Reflected or non stored XSS**). **Stored or Persistent XSS** is when a popularly used site has a script embedded in it that actively pursues anyone that interacts with it or the site(depending on how involved of a script it is).

Firmware is the OS on the hardware devices.

Virtualization

Virtualization vulnerabilities:
-code injection
-information disclosure
-local privilege escalation

VMs are their own running machine, It's not easy but it is possible to jump from one VM to another on a hyperV. Once you escape a VM on a system you have a lot of control.

Cloud Specific vulnerabilities
-nearly all organizations use it to an extent.
-A majority of cloud infrastructure is unpatched.
-Anyone can attempt to connect to it and anyone can attempt to DOS it.
-Could even bypass authentication through a lot of means.
-Faulty configurations.

Supply Chain Vulnerabilities

Anyone who builds the hardware and software is part of the supply chain.
Service providers can be a vulnerability as they can be a target for an attack.

Third parties are used everywhere so many organizations have security audits with all of their third party service providers.

Why there are vulnerabilities:
-The hardware could have malware in it that can be used to attack your organization. A trusted relationship with vendors is key but treat all devices as if they are untrusted.
-the software could update automatically(or just upon install) and infect your computer. Could also break your environment.

MISCONFIGURATION VULNERABILITIES

Wireshark is a packet capture software

Opening ports allows someone a little bit of access to your servers. Firewalls manage ports.

Firewall administrators need to constantly be auditing their system.

Mobile device management

Sideloading is when someone has installed unauthorized software(pokemon go hacking or jailbreaking)

Storage segmentation is when mobile devices store corporate databases and personal databases separately.

Containerization is the act isolating corporate applications from the rest of the device

2.4 Malware

…

Physical attacks

Old school security
If they can physically touch it then it isn't safe.

Brute force is forcing something open using strength, IE breaking a window or a door.

RFID cloning is when they copy access codes onto a blank smart card and then use it to scan into buildings.

Environmental attack is to attack the area around the system, IE Cutting off the power or HVAC

Network attacks

Denial of service is when you can't access the server
Can happen from plugging switches into each other causing a loop or a loop in the transport protocol transferring too much info making the server go down.

Distributed denial of service is when botnets are used to attack the network from all over. Botnets are centralized to one system but located everywhere. Also known as a asymmetric threat as the attacker is far outnumbered by the target network.(commonly uses NTP, DNS, or ICMP request)

DNS attacks send a dns request over and over to make the network send back a far bigger packet of information.

DNS cache poisoning Remapping a domain name to a rogue IP address

Reflective DDOS Utilizing third-party servers to reflect and amplify attack traffic towards the target

DNS Poisoning(spoofing) attacks- DNS servers are well protected so they modify the host files on the client and modify the DNS query to make it send all queries through a process of the hacker's choice. The hacker would have to sit in the middle of the transfer to send them to a malicious site.

Domain hijacking is when you find credentials or just gain access to the domain registration. They would then be able to edit the domain information. This allows attackers full access to the system.

URL hijacking is when you use a domain that is similar to an original domain(like a misspelling). Can use their domain to redirect traffic from the original site and influence customers to use their malicious software.

Wireless Attacks

*802.11 wireless has a number of management features:
-Can be packet captured.
-it is unencrypted :(if you are close you can access
-provides **management frames**(information about the connection for admin purposes)

Deauthentication attack is when you disconnect a device from a wireless network over and over using a Airecrack -ng command while tapped in.(needs to be local to the AP)

IEEE addressed this with the 802.11ac by encrypting management frames that allowed deauthentication attacks to happen by unauthorized users

Wireless jamming is when you send data packets that designed to be too big to disrupt the wireless service.(needs to be local to the AP)

An **initialization vector (IV) attack** is an attack on wireless networks. It modifies the IV of an encrypted wireless packet during transmission. Common in WEP.

On-Path Attacks

Formerly known as **man in the middle**

ARP (Address Resolution Protocol) Poisoning is when an attacker hides in the middle of a router and workstation and sends a mac request to the router and terminal and tells them that the attacker's address is the router or workstation. That means they can see anything that comes though.

On-Path browser attack is when they track your online browser usage.

Replay Attacks

USeful information is always transmitted over the network.

This attack requires raw network data, like from a network tap or ARP Poisoning.
Once obtained they can send it back to the network and it will replay.

Passing the hash is a common replay attack when an authentication request is sent to a server but the man in the middle obtains the hashed token or password and then sends back the hash to the server and obtains the target user's credentials. Can be stopped with salt.

Cookies help with tracking and session information

If an attacker obtains a victim session id they can log into a website under the victims ID. The session ID is contained in the Header. Can be sniffed out by a packet capture software like wireshark, XSS. modifying headers(like with firesheep), or modifying cookies.

HTTPS secures this problem

Malicious code

Malicious code bad :<

Application Attacks

Injection attacks when an input can be injected with an attackers own code

Extensible Markup Language (XML) a flexible text format designed to describe data for electronic publishing. An **XML injection** attack involves sending malicious XML content to a Web application, taking advantage of any lack of input validation and XML parsing.

Buffer overflow is when you overflow the input so that an input overflows and then overwrites into the next column on the memory. Relatively difficult to find and use.

Replay Attacks see earlier

Privilege escalation is when you access admin credentials through exploitative means.

Cross site request forgery(CSRF(SEA SURF) or XSRF)-one click attack or session riding. uses a hidden link that uses the trust between the victim and the server they are trying to connect to(If you click on a link that redirects you to your bank and you already logged in and then the bank then receives the code from you which would send all your information to the attacker that sent the link.)

Directory traversal like when you change the URL to look for certain files or directories in the system beyond the application. Can be bad if you host your site on a server or machine with other files.

Cryptographic attacks

The key is the difference between secure and unsecure data. In order to get around the key they have to attack the safe(the actual ciphertext) to see the data without the key. We trust a majority of the modern algorithms so we look at the implementation of the algorithms to attack instead.

Birthday Attack-relies on similar hashes or cipher text in order to decrypt messages. Found through collisions and brute forcing hashes to find duplicates. The way to stop this is with larger hashes. The

bigger the hash the harder to crack. MD5 is now deprecated. SHA 256 is now the common hashing algorithm.

Downgrade attack- forcing a system to use an older less secure system or protocol. Most common is **SSL Stripping**(one on path attack vector and a downgrade attack.) Which works by making the HTTPS into HTTP, making their connection insecure.

PASSWORD ATTACKS

Spraying is when they use the top 3(or more depending on lockout or alert criteria) most common passwords on every account in the system.

Brute force is when they use every combination of password or hash to gain access. Takes a very long time.

Indicators of Compromise(IoC)

Indicators:

-unusual network activity
-hash irregularities
-Irregular international traffic
-Changes to DNS data
-Spikes of read request to certain files
-account lockout without logging in.
-when admin is mysteriously disabled
-clone accounts in different locations
-blocked content means malware is trying to stop patches to prevent being eliminated
-geolocation login/logout log data
-unusual spikes in traffic at unusual times or through unusual services.
-files transfers when nothing should be happening
-resource inaccessibility
-out of cycle logging: logs popping up at a weird time, like when updates happen at weird times rather than their regularly scheduled updates.
-Missing logs to hide themselves.

2.5 Segmentation and Access Control

Physical logical and virtual segmentation
Devices,vlans, and virtual networks respectively.
For security purposes it is important to divide information up so one area can't have all the data and one area can't be exposed for everything.

ACL(Access control list) lists the permissions of each user. OS' use ACLs for their file systems.
Allow list - nothing can run except those allowed
Deny list- anything can run until the ACL see's something it doesn't like.

Windows has network zones and on path running which only allows certain areas to run and can prevent another from running

Mitigation

Patching known vulnerabilities is the best way to mitigate risk. Make them continuous.

Encrypt the file system itself. Windows **EFS** is the Windows OS File Encryption System
Full disk encryption uses Bitlocker on PC and FileVault on Linux to make the entire disk encrypted.

Use of a **SIEM** to consolidate all built in logs and give reports of all data.

Least Privilege means the rights and permissions of a user are based on their job and their job only. No one would be an administrator, would only sudo it upon necessary through a separate authentication process.Limits the scope or surface area of an attack.

Configuration enforcement runs a check for the OS version, **EDR(endpoint detection and response)**, status of firewall and EDR, and certificates. If anything is off it will send it to a quarantine VLAN to make changes in order to meet the network's standards.

Decommissioning data is when you need to end the life cycle of a data storage device. Follow protocol for disposal and make sure no information is still on the device(IE: USB, SSD, HDD)

System Hardening

Security updates are most important in hardening.
-User accounts should all have complex passwords and each account should be limited to what they need to do their jobs.
-AntiVirus AntiMalware
-Encrypt Data

The system needs many different programs to function as a **defense in depth.**

EDR(Endpoint detection and response) Scaled to meet needs. Can detect a threat through behavior analysis, machine learning, and process monitoring. Lightweight on the endpoint. It can then respond to threats. Very advanced.

HBFW(host based firewall) Software firewall for personal use. Monitors incoming/outgoing application traffic.

NGFW(next gen firewall) is the most advanced firewall.

CLOSE ALL UNNECESSARY PORTS!

Nmap scans ports to show which are open on a system.

3.0

3.1 Cloud infrastructure

Iaas,Paas,Saas,etc

Security is well documented by the cloud provider to tell who(customer or SP) is responsible for which aspect of security. Called a **responsibility matrix**.

Hybrid cloud uses different cloud providers, while it's more secure it's more complex and would require two separate manual configurations. It can have a big mismatch in configuration if done wrong. Can be leaked while it transits data from one cloud to another as it travels over the internet. Be sure to configure secure transit correctly.

Third party cloud based services like firewalls require a vendor risk management policy to mitigate risk. Always watch these third parties for sudden changes or mismanagement. **Third party assessment** relies on looking at an organization's entire supply chain for vulnerabilities.

Infrastructure as code(IaC) describes an infrastructure as servers, networks and apps as code. The code can then be duplicated and built out on different instances on different clouds.

Serverless architecture - FaaS(function as a service) apps are separated into small functions. Like Event triggers and alerts. Short term stuff.

Monolithic applications are the legacy form of all applications. Now we use cloud applications to make it much more efficient.

API is the glue of the microservices. They do minor automated functions based on need. Opposite of monolith infrastructure, small and efficient.

Isolation is when a **physical** separation between computers prevents computers from communicating with each other. Requires a separate layer 3 device(IE Router). They are **air gapped.**

VLANs allow for network segmentation through your switch. The VLANs can't connect to each other so it is more efficient than having two separate switches in isolation. Far more scalable as well

SDN(Software Defined Networking) Planes of operation are Data, Control, and Management. Splits them into their functions that can be coded and made into usable software for our cloud.
PLANES:
Infrastructure/data plane - Processes network frames and packets. Forwarding, trunking, encrypting and NAT.
Control plane- Manages action in the data plane. Routing tables, session tables, and NAT tables. Dynamic routing protocols.
Management/Application Plane- the way we connect to it and code within using a CLI.

Other infrastructure concepts

Cloud based security is centralized and cheaper. Scalable

On-Premise is more expensive but you have complete control over everything. The IT team is well trained on the entire system as they configured and developed it for themselves. Most of the time decentralized throughout an organization's many locations.

Centralized has a single point of failure

Devices that are integrated in the network and you interact with everyday are called **Internet of things(IoT)**. IE automatic lights, ring camera, smart watch, auto heating and cooling. Security concern.

SCADA/ICS- supervisory control and data acquisition system. Centralizes all data from large machinery. Allows full system control and monitoring of each machine.

RTO(real time operating system)/Deterministic Operating System- Focusing all of its power into one function is the reason it exists like the brakes on a car or a ventilator in the OR.

Embedded systems are systems that have one function and one function only, like a clock in an apple watch.

HA (high availability) is used to make sure that if one fails it will always have a second option for power or sourcing.(like the ventilator has a backup cpu in case one breaks.) A step above redundancy.

Infrastructure considerations

System uptime is available. We want to make sure they are available but only to the right people. We spend a lot of money on ensuring secure availability.

Resilience: can you maintain availability? Can you recover? How quickly?
MTTR(mean time to repair) is how long it will take to repair a system or return from downtime.

Cost:
-Initial installation
-Maintenance(can go to the manufacturer or internal)
-Repair costs
-Tax implications

Responsiveness, we want things back as fast as possible as humans. Hardest to quantify

Scalability is based on how much we use something. **Elasticity** is how fast we can scale and descale a system/app.

Ease of deployment is based on how many things and moving parts go into app deployment. Cloud based infrastructures have the easiest deployment.

Risk transference is when you transfer penalties to third parties like insurance.

Malware infections require back ups to be installed, about an hour for a full OS restart or ten minutes for a corporate image backup.

3.2 Secure infrastructures

Every network is different but contain similarities
Firewalls can segment networks.
Other **secure technologies** are honeypots, load balancers, and jump servers, and sensors

Security zones allow us to logically assign computers on a network based on rules. Internal vs external zones. Internal can have zones in it like internet servers, databases and screening zones.

Attack surface is any vulnerabilities a hacker can get in through. Possibly an app, human error, open ports or even authentication spoofing.
To minimize the attack surface we must:
-audit code
-monitor traffic
-block ports and configure firewalls

Protect physical cabling from tapping, this is why we should include application level encryption to block anyone who may tap into the network.

Intrusion Prevention

IPS(intrusion prevention system) watches the traffic in real time and blocks that negative traffic.
IDS(intrusion detection system) alerts and watches but does not block traffic.

Fail open- when there is a crash data will continue to flow through it.
Fail closed- when there is a crash the data will be stopped from flowing through it.
Think of an emergency door that remains open in an emergency.

Passive the monitoring system isn't inline and wont cause downtime if it crashes but also has limited access. More common in IDS
Active is inline in front of the Switch, gives it more capability but can cause more downtime. Default config for IPS

Network appliances

Jump servers - allow you to jump into the private network from an external client using a device on the inside of the network called a jump server.

A **Proxy Auto-Configuration (PAC)** file is a JavaScript function that determines whether web browser requests (HTTP, HTTPS, and FTP) go directly to the destination or are forwarded to a web proxy server.

A **proxy server** sits in the middle of two devices and makes requests on behalf of one of the two. Used in a private server to allow clients to make requests to the internet(forward proxy). Contain firewalls and content scanning.
Explicit Proxies require configurations
Transparent proxies have no configs and the user has no idea there is a proxy in place.

Network Address Translation (NAT) is a process used in routers to modify IP address information in packet headers while in transit. It enables multiple devices on a local network to share a single public IP address for accessing the internet, conserving global IP address space and enhancing security by hiding internal IP addresses

Most proxies in use are app proxies

Forward proxy is common to be found in internet use from a private network.(private to internet)
Reverse proxies are used when a user on the internet makes a request to a web server, which protects the web server. Can act as a caching service for the web server.(internet to private)
An **open proxy** is a third party proxy that anyone can use which has many security concerns.

Load balancers split up the resources among the servers. Users don't even know it's there.
-Active/Active load balances manage loads across all servers. Distributes the network load evenly from its own tcp protocol. SSL offloading includes meaning it can encrypt and decrypt data.
-Active/Passive is when only some servers are being used but some are not. The passive servers can be called upon an outage in an active server.

Sensors and collectors are used to compile statistics and send them to a collector which can then be analyzed. **SIEMs** are a powerful tool used with sensors to monitor data, traffic, and network statistics.

Port security

Security on the individual ports on a switch or through a wireless network.

EAP(extensible authentication protocol) works with both wireless and wired traffic systems. IEEE **802.1x(NAC)** is a standard for authentication used with EAPs.
802.1x is used with RADIUS, LDAP, TACACS+, and kerberos

A request from the authenticator is called an EAP request,

An **authenticator** stands in between a client/supplicant and an authentication server(which contains the login data and algorithms for logging in.)

Firewall types

Designed to control traffic flow between two points.
Control inbound and outbound traffic. Can stop use of websites.
Perfect place for antimalware and antivirus
Traditional Network firewalls use OSI layer 4 over TCP/UDP
NGFW use layer 7(application layer)
Can include a vpn.
Many firewalls operate as a layer 3 device(router) and can sit on a network gateway and control traffic in and out. Can provide NAT(network address translation).

UTM(unified threat management) is an all in one threat fighter. Contains URL filter, malware inspection, spam filter, CSU, Router/switch, firewall,IDS/IPS, bandwidth shaper, and VPN Endpoints. Can only use a few before the device can slow down.

NGFW(next gen firewall)- sometimes called application layer gateways. Provide full packet decodes of any traffic into or out of the application. Can monitor SQL server, stop viewing of videos or sites, and block certain traffic. Includes an IPS. This also means it has a content filter.

WAF(web application firewall) Analyze input into web based apps. Protects the application. Common in stuff using HTTPS and HTTP. Commonly used in conjunction with a NGFW

Secure Communication

VPNs allow you to securely connect to a private network through a public network like the internet.
^NGFW provides this capability for us.

Tunnel mode works by encrypting all data in the IPheader and data inside IPsec wrappers and then a new IP header is made to be able to send the traffic properly and then decrypt it once it reaches its destination.

Tunnel Mode provides end-to-end security by encrypting the entire IP packet, while **Transport Mode** only encrypts the payload of the packet.

Most of the time we use **SSL/TLS VPN** and have almost no firewall issues over port 443.
An SSL VPN is used for remote access to a corporate network.
Does Not require authentication to use.
Sometimes called **remote access vpn**

SIte to site(IPsec) VPN communication uses two firewalls that have VPN concentrators that automatically connect a remote site to a central site or HQ.

SDWAN(software defined networking in a wide area network) is specifically designed to address issues with cloud based apps. Requires wide area networks that allow access from wherever you happen to be. Has to be configured with almost no geofencing. Connects all sites and data centers by allowing them all to have equal connection to the cloud.

SASE(secure access service edge) Next generation VPN that allows for efficient communications with web based apps in the cloud. Security technologies are now all cloud based. You can sign on from wherever. Used with SD WAN

A **remote access service (RAS)** is any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices

3.3 Data

Data to secure(sensitive data):
-Regulated data means it is governed by a third party. Like credit cards(PCI DSS) or federal data standards.
-Trade secrets need to be protected as they are closely guarded secret to companies
-Intellectual property is protected using copyright and trademark law. Usually public knowledge.
-Legal information(PII in it is sensitive)
-Financial details

Data types
Human readable(self explanatory)
Non human readable(barcodes, images, encoded data)
Hybrid(json,CSV,XML)

Classifying sensitive data needs to be based on how sensitive or important the data may be. Like license plates vs health history.
Adding permissions, different processes, and restricted areas are ways we separate different classes of data.

Proprietary data is data owned by an organization and unique to it. Not found outside of the company.

PII(personal identification information)-like name, DOB, mother's maiden name, Biometric, etc anything that can be related back to you.
PHI(protected health information)-health status and records that are protected by HIPPA

classifications:
Sensitive: Intellectual property,PII,PHI should always be protected
Confidential:Very sensitive must need approval to view
Public/unclassified:No restrictions
Private/classified/restricted: restricted access may require an NDA. Most restrictive.
Critical:needs to always be available.

States of Data

Data at rest is when data is simply stored.(HDD,SSD,USB)
-Applying permissions like an access control list to have security on data

Data in transit is when data is being transferred over a network.

System RAM holds onto the data and processes it in the CPU. When it's in these two it is not encrypted and is called **data in use.**

Data sovereignty is applied to data that is stored in a country. The data should be stored in regulation with the nation it is stored in.

Geolocation shows where users and data are physically located. Uses info like gps, 802.11 info, or mobile provider data.

Protecting data

we enroll geofencing policies to stop users from restricted areas from accessing a network.
Organizations go out of business without data, that is why we make money to protect it.
Data is literally everywhere.

Protection methods:
-encryption
-security policies
-permissions

Encryption turns Plaintext into a ciphertext using a cipher. You need a key to decrypt it.
Confusion is when the original data is very different from its encrypted state.
Hashing represents data as a short string of text. It's the fingerprint of data. We commonly store passwords using a **hashing function** to ensure confidentiality. Verifying downloads is another function of hashing which provides integrity. We trust our current algorithms not give us collisions.

Segmentation splits up databases to prevent a total breach.

Permission restrictions - starts with authentication to ensure proper usage. Additional security is applied once they log in and decide what the user can do, also known as authorization.

Remember **obfuscation, data masking, and tokenization** because those are other data protection methods.

3.4 Resiliency

Redundancy doesn't mean available
HA(high availability) means something is always on and always available.
If one system fails you have a second system that swoops in and takes on its load.
There is extra cost that comes with high availability.

Server clustering is using many servers to make up a central server system. You can increase and decrease the scale of it at will.
Load balancing is similar but uses one load balancer to control each server. A server cluster knows of the other servers in its cluster but a load balancer the servers are not aware of its counterparts. The load balancer is the central point in which traffic gets distributed. Can be added to or minimized upon need just like server clustering

Site resiliency is physical resilience for a disaster. This would include something like **DRP** or a **BCP.**
Types of recovery sites
-**hot sites**:contain all of the data from the central site in a separate location. Exact duplicate and can bring back central sites very fast
-**warm site:** Mid range between a cold site and a hot site: contains some equipment or data used for recovery but some will still have to be recovered from the disaster/central site in order to create a full recreation of it. Just the equipment needed to get going in recovery.
-**Cold site**: just a physical location that requires all of the equipment needed to provide resiliency for a disaster. Any databases, servers, or systems that are needed for functionality will have to be transported here without incident to make a full recovery. The slowest of the three sites.

Recovery sites must be in a physically separate location incase of physical disaster.
This can be a huge logistical challenge that can amplify over greater lengths

Platform diversity is important because each OS has different vulnerabilities. Using each OS can limit exposure to each vulnerability.

Plan for cloud outages by making backup systems on other cloud providers(AWS or Azure). Increases uptime and availability.

Plan for every Contingency

COOP(Continuity of operations planning)- not everything goes to plan, a disaster, big or small, can cause disruptions in any service at any time. When technology isn't available we need to have a physical backup method of services. Like writing down credit cards when POS systems don't work.

Capacity planning

Has to meet the supply and demand of the application.

Plan capacity for:
-people(prevent understaffing and layoffs)
-technology(think of working with a load balancer and seeing how many servers and service you need)

-Databases(cloud or physical hardware)
-cloud services(Easiest to scale for capacity)

Recovery testing

Testing yourself for an event, does not use actual systems.

Tabletop exercises are cost effective solutions that allow you to talk through the steps of recovery as a group of people. Allows each group of people to be represented in a drill-like setting and provide input.

A **Failover test** is used to see if a redundant system kicks in upon being needed. Checks the fail safe devices for any failures to switch over to redundant systems. Routers, firewalls, and switches all have built-in failover processes.

Simulations, like phishing simulations, test users and administrators on their cyber skills and we can see who clicks on links or engages in AUP violations. Also tests if our auditing systems work upon being activated in the simulated test, like if the link is clicked on.

Parallel processing allows for multiple CPUS or cores that allow for simultaneous processing. This gives us more efficient processing and allows for redundancy incase of computing failures or processing corruption.

Backups

Backups are incredibly important
Allow quick recovery

Many different implementations:
-Total amount of data
-Type of backup
-backup media
-backup storage
-backup and recovery software
-schedules for backups

Onsite backup is when data is onsite and ready to use. Cheaper to use

Offsite backup is when you pay for storage of data at a separate physical location. Used alot in long term storage

Many organizations use a mix of the two.

Frequency of backups is determined by how important and how much you use this data. Many backups can happen on different days in order to be efficient.

Encryption is important but there are many other security concerns we have to plan for with back ups, including physical theft. Cloud back ups are generally required to be encrypted.

Snapshots are backups for VM's that create entire copies of the VM. Can be pulled up later when needed.

It's important to test backups to make sure they can be used for proper recovery.(Key term: **Periodic audits**)

Replication is copying data as it comes in and storing it in an entire secondary identical system. (hot sites)

Journaling is needed when storage gets corrupted while in transit or during the initial storage process. Corruption recovery is a time consuming process so we use journaling to make a back up of the data in a journal on the drive and then write it to the database. The database can recover data that gets corrupted during the storage process.

Power Resiliency

Power Resiliency is planning for power outages.

We can mitigate both short term and long term power concern risks.

UPS(uninterruptible power supply) a usually low voltage device that uses battery power to keep systems running for a short term period.
-Offline UPS are for when a system goes offline is will kick in
-Line interactive UPS is one that will increase the voltage if the main powerline loses a little bit of voltage.
-Online UPS always runs on battery backup.

Batteries on UPS are limited so make sure to research what you will need. Can also even have Ethernet and telecable functionalities if need be.

Generators are fuel based power supplies. They have slow start ups so UPS can be used in conjunction with them, until they get everything up to proper power supply needs. Generators are long term power backups.

4.0

4.1 Secure Baselines

The security of an application should be well defined and documented.
-all apps must all follow the baseline
-firewall settings, patch levels, and OS file versions
-may require constant updates
Integrity Measurements check for the security baseline.

Many manufacturers or organizations have created security baselines for their products. Many of the systems or technologies you use have different baselines created for them.

SCT(security compliance toolkit) is a microsoft tool that helps you figure out and config your security settings for your whole system.

Deploy baselines - Many are default but you may have to configure certain rules through active group policies,mdm, etc. Automating this process is key to efficiently managing and deploying security baselines

Managing baselines is simple as most of them will stay as is for a while, but sometimes vulnerabilities are made or found that can require updating baselines to accommodate.

Test your baselines to ensure they work with your system properly. Once again continuous auditing is key.

Hardening Targets

When installing an OS, the default configs are usually not very secure. Each OS manufacturer will produce a hardening guide that gives recommendations on hardening the system.

The manufacturer of mobile devices apply security patches through software updates
A mobile device manager(MDM) helps monitor and push out security updates for mobile devices

Workstations need hardening as well. The OSs(WIndows,Mac, Linux) compile an update of security patches and release them all on one day a month. Automating these is easy to do and allows easy testing. Good security practice is to remove all unnecessary software on the device.

Network Infrastructure hardening consists of hardening Routers, switches, firewalls, etc. Configurations are needed upon implementation. Check for updates and patches through the manufacturer.

Cloud infrastructure hardening is reliant on authentication(the keys to the kingdom)**.** Uses the concept of least privilege within the cloud. EDR(endpoint detection and response) is needed on Cloud based infrastructure. Backing up these systems to a separate cloud is very important.

Server hardening consists of OS updates or service packs and security patches. Also User accounts and managing these accounts. Set policies within the server or firewall to limit access. Should also always include EDR, IPS, or some kind of client based detection system.

SCADA/IDS is used for large scale manufacturing systems. It's a centralized system for managing them. Provides real time information and system control. These devices are the most secure devices, most of the time on their own isolated network with no access to the internet.

Embedded systems can be difficult to update, however some are as simple as clocks and televisions. Applying patches is the only real way to harden it.

RTO(Real time operating system) is when individual operations are needed to be isolated from the network in order to function. It usually has many things going on but will focus its energy on one thing when instructed to. Based on real time operations.(DUH)

On **IOT devices** patching is crucial once again. Segmenting IOT devices to their own network is another hardening strategy.

Securing Wireless and Mobile

You perform a site survey when you want to test a new or disfunctional wireless network. It allows you to understand how your network will perform and how other networks around you may be affecting your signal. Allows you to find access points. Work around the existing wireless access points(to stop conflicting frequencies.) Plan the wireless layout to achieve the best connection.

A heat map is a map of how well each area connects to the network, based on signal strength for the WAP.
Use a wireless survey to see signal coverage, potential interference, or use tools that can help monitor more network capabilities.

Spectrum analyzers allow you to see all frequencies. They can be used to see any possible frequency conflicts.

A **mobile device manager(MDM)** can be used on **BYOD or Company owned Personally enabled(COPE)** devices. Allows a system administrator to roll out policies or make sure of application installation. Can set policies like no cameras or restricted access to the net. Can control the whole device remotely or “partitioned” or partly controlled.

BYOD is the most difficult to secure.
CYOD is **choose your own device**, still corporate owned

Cell networks produce traffic monitoring, location tracking, and worldwide access concerns.

WIFi have concerns of data capture(by means of LAN), man in the middle attacks, and DOS attacks

Bluetooth devices also produce frequencies that can be used maliciously. Never automatically connect to a bluetooth device.

Wireless security Settings

An organization needs its data to be encrypted on its own network. This is why we only should allow authorized users into it. We need to first authenticate(password or MFA) them then authorize them for access to the network.

All traffic should be confidential and have integrity. Encrypt the traffic outbound and inbound and ensure integrity through an **MIC(Message integrity check)**

WPA2 has been traditionally used to send traffic across the network or internet. It relies on a handshake that provides a hash called a **PSK(pre shared key)** to ensure secure connection. Over time hackers have found out that you can go offline and take that hash and put it into a brute forcer to crack the hash and make it readable. Now anyone with the hash can access the network

WPA3 is the updated WPA2 that introduces new tech to block this vulnerability. Uses the **GCMP** that uses a block cipher to create a stronger encryption. Provided confidentiality with modern AES. Has its own **MIC** with th**e Galois counter mode code.**

CCMP(WPA2) vs GCMP(WPA3)

SAE is the updated version of the WPA2 handshake protocol. WPA3 changed the PSK authentication process. This includes mutual authentication and creates a session key like mentioned earlier. Prevents the Hash being shared in the handshake. This new method is called the **Simultaneous authentication of equals(SAE).** It relies on A **Diffie-Hellman ephemeral(DHE)** for each session id, which is because each session ID is temporary. This is included with the latest IEEE standards, like 802.11, and called a **dragonfly handshake**.

Wireless authentication methods:
-Use of PSK(like wireless network password)
-802.1x credential authentication(proving a User ID and Password, like at the office)

Different configs:
-open system
-WPA3-personal/PKI
-WPA3 Enterprise

AAA framework
-Authentication
-Authorization
-Accounting

RADIUS(remote authentication dial-in user service) is one of the most popular AAA protocols. Heavily supported. Any login attempt or network traffic can be run through the RADIUS server.

Network access control(NAC) means no one can gain access to the server unless they provide credentials. 802.1x provides this for us. You can use this in conjunction with a RADIUS, LDAP, or TACACS+. Centralizing this onto a AAA server allows us easy control over the protocol and provides an easy way to add/remove users.

EAP allows us to embed authentication into the 802.1x process.

AAA servers are also known as authentication servers.

Application Security

We are constantly tasked with applying patches and balancing time/quality.
Testing is done in the **Quality Assurance(QA)** process
Input validation ensures that any unexpected data will not be interpreted as a command.
Fuzzers are automated processes that put random data into input fields to allow the developer to see if anything messes up.

Cookies are information stored in the browser. They are used in containing Session IDs and tracking. There is a secure set of cookies only sent over HTTPS. Anyone can read it so sensitive information is never secured in them.

One way devs test their security is through **SAST(Static application security testing)** like with a **static analyzer**. Can find buffer overflows, database injections, etc. Can't identify all vulnerabilities, like cryptography implementation errors. Always check it for false positives.

Code signing allows us to ensure integrity from downloading apps off of developer. We use a DSA hash to verify it that is the proper install.

Sandboxing for apps is used to build or test an app in an environment with only its dependencies.

Many developers build monitoring into their application. Allows for real time monitoring and find vulnerabilities in their app.

4.2 Asset Management

The purchasing process is a highly formal process for acquiring or selling goods or services.
-starts with a user request
-includes sign offs from other departments
-negotiate terms and services
-purchase and invoice

Once assets are received they are put into an **Asset Tracking System**(a big inventory for devices). Associates the device or system with a person and then that can be used for tracking. We also use it to track asset life cycles. The tracking system will also allow us to classify systems, like hardware/software. Allows us to issue tickets to devices. Includes enumeration of all of the parts of the device. We can add a tag to it to label it, like a barcode or qr.

Media sanitization is about clearing off all data off a storage system or device. This is called decommission or system disposal. There are different sanitizing methods depending on different use cases. Common in reuse of storage devices.

Physical destruction is as it seems. Physically breaking the drive

Degaussing uses a strong magnet that wipes the drive.

Some Companies even incinerate their drives

A **certificate of destruction** is a guarantee that all data that has been given to us has been destroyed.

Data retention relies on regulatory compliance. This could be like how long financial data and emails have to be stored. This should be tied to a backup and disaster policy.

4.3 Vulnerability Scanning

Vulnerability scanning tests for potential of attack on a system
A port scan is a common vulnerability scan.(nmap)
Test scan internally and externally
Nessus is a popular GUI for network vulnerability scanning.

SAST is for application scanning

Fuzzing is another application test, common fuzzer is the CERT BFF

Package monitoring is reliant on monitoring and verifying all inbound and outbound packages. You should test these before implementation.

Threat Intelligence

Research all of your threats.

OSint (open source intelligence) is publicly available and a good place to start looking for threat vectors and vulnerabilities that could apply to you.
Proprietary/third party intelligence is when you hire a third party to know and monitor for any threats that affect any part of your organization.
CTA(cyber threat alliance) is a group of organizations that all gain knowledge on threats and send them to be approved by the CTA. Once approved it is graded and sent to all the members.

The **dark web** is a secret browser used to find the lower levels of the internet. It can be used to find all sorts of intelligence.

STIX (Structured Threat Information eXchange) a common language for describing cyber threats

TAXII (trusted automated exchange of indicator information) is a dedicated transport mechanism for sharing cyber threats and vulnerability information.

PenTesting

To simulate an attack.

Look into the NIST pentesting documentation to learn more.

Rules of engagement are a formal list of rules to lay out the scope and purpose of the PenTest. Could define objectives, time, and detailed breakdowns of allowed systems.

Try every vector you can to the best of your ability to test the limits of your security. Once you gain access you want to move up in rank through lateral movement. This would be where you could install a system of access like a backdoor for you to gain access whenever you want(persistence).

It takes time to fix a vulnerability

Analyzing Vulnerabilities

Levels of severity:
-Critical
-high
-medium
-low
-informational

False positive is given because it flags something that is not faulty.
False negative is when a vulnerability is present but it is not flagged.

Prioritizing vulnerabilities are based on levels of severity. The **CVE(common vulnerability enumeration)** list is a list of all vulnerabilities and scores them. You can base your levels off of theirs or you can change priority based on personal needs.
NVD(national vulnerability database) is synced with the **CVE**

Always look into the manufacturer after identifying a vulnerability

Your **vulnerability scanner** is going to gather all of its vulnerabilities and give you a summary of all types of vulnerabilities. Can perform application scans as well. Some can even detect vulnerabilities in firewalls, switches, and routers.

An **exposure factor** is represented as a percentage that is based on how exposed and how easily hacked certain vulnerabilities can be. The percentage of the assets value that would be loss if hacked
SLE = ExFac * Asset's value

Use the **CVSS(common vulnerability scoring system)** score along with your own exposure factor when making priority hierarchies.

You can't patch everything all at once. The process of deciding which patches get patched first is called **risk tolerance**. (Which one is more important to patch?)

AIS(automated indicator sharing) is a US government initiative that allows cyberteams to share any indicators or vulnerabilities related to breaches with a common gov body to allow all cyber engineers to learn about them.

Vulnerability Remediation

The most common mitigation technique is knowing what is vulnerable and applying a patch.
Scheduling patches is a priority in IT
You often have to work with unscheduled patches for stuff like zero day attacks.

You can **mitigate the risk** through a Cyber Security insurance policy. It doesn't cover everything but is important to have in the modern world.

Segmentation(look at earlier notes)

Compensating control is when the optimal method is inaccessible or unusable and you use a separate method to try and make up for that vulnerability.

Removing all vulnerabilities is optimal, but not everything can be patched. This job is a balancing act. Should we make an exception or an exemption is a question we must ask when applying patches with issues.

An exemption is when a group decides on leaving out a patch.

Validation of remediation happens after the patch is finally applied. You now need to retest your system and scan to make sure the vulnerability has been fixed.

A reporting system helps keep track of patches and rollouts. These need to be continuous.

4.4 Security Monitoring

Systems are one thing we can monitor
-we can check account authentication and login data
-we want to make sure servers are running smoothly and backed up
Applications we monitor are

-Availability
-Data transfers
-Security notifications from the dev
Infrastructure we monitor
-Remote Access systems
-Firewall and IPS reports

The **SIEM(security information and event manager)** centralizes all of your logs and allows you to easily display and monitor them together.. Can create reports and alerts from it.

Organizations take part in active scanning and testing to ensure the changing landscape of threats are constantly being monitored.

Actionable reports give us a clue of what to do next

It takes an average of 9 months for organizations to contain a breach
Archive data over an extended period. You may be mandated to archive for business or security purposes by the law.

Alerting sends real time notifications for certain triggers. Actionable data should be used to keep the right people in the loop and enable quick response times. A common reaction to alerts is **quarantining** the alerted device by logically separating it from the network.

Security Tools

SCAP(security content automation protocol) allows security tools to work together automatically

Apply security best practices to all systems in your environment.

A **benchmark** is typically a set of standards or guidelines that provide a point of reference for measuring performance, security, or other attributes of a system. In cybersecurity, benchmarks often refer to specific configuration standards developed by organizations like the Center for Internet Security (CIS) to ensure best practices for system security.

Agent-based systems are always running and requires constant maintenance of system configurations
Agentless systems simply perform a check over the system then disappears, does not require constant running but won't update or alert while offline.

SIEM(see earlier)

Antivirus/anti malware detects and prevents them functioning. Commonly seen as interchangeable terms

DLP(data loss prevention) prevents any data from being sent off of the server. You can classify any data as sensitive and the DLP will block it from leaving

Simple Network Management Protocol (SNMP) is a protocol used for managing and monitoring network devices such as servers, firewalls, and routers. It utilizes a **Management Information Base (MIB)**, which is a database containing **Object Identifiers (OIDs)** that represent various pieces of data. SNMP typically uses UDP port 161 for sending and receiving requests and responses

SNMP requests statistics from devices in the network, and these requests are called **polls**. They are used to monitor various network statistics.

An **SNMP trap** is an alert sent from an SNMP agent to an SNMP management station. These traps notify the management station of significant events or changes. SNMP traps are sent over UDP port 162 to the management station, where the alerts can be processed and acted upon.

A way to gather additional network detail is through **netflow**. It Monitors traffic and application use.
It is used through a probe that is either tapped or wired into a switch through a SPAN(switch port analyzer). Then the logs are sent to a SIEM or separate reporting app.

4.5 Firewalls

Network based firewalls and NGFW(see earlier)
They encrypt traffic
Manage access control

Firewall rules
-Logical path (top to bottom)
-Can be very general or very specific
-Implicit denies
-ACL
-many other minor factors like time and location

A screened subnet is an off path network that allows in outside traffic to be scanned before entering the internal network.

IPS rules are generally integrated into the NGFW. Some are signature based and look for specific actions and some are anomaly based and block traffic based on known malicious behavior patterns.
There are thousands of possible IPS rules and you can set broad or specific rules based on the needs for each group.

Noise is another name for a false positive, usually in a large service like an IPS

Web Filtering

Web filters are designed for things like inbound/outbound data or browser restriction.

URL scanning is used to filter out certain web pages. They group together websites based on **URIs(uniform resource Identifier)** which contain all similar URLS. often built into the NGFW.

The control of the URLs may not be functional from a local firewall, we can use an agent based firewall to manage the content on a remote device. Its a software based firewall that connects to a central controller which then manages content filtering

Proxies are servers that sit in between a private network and the internet.(see earlier)

Some block rules:
-URL websites

-Website categories
-messages into logs

Some filters might evaluate the **reputation** of a site to allow or deny access to the site. Risk types would be trustworthy, low risk, medium risk, suspicious, and high risk. You can make a rule to block certain types of risk.

DNS filtering configures the DNS to not allow the user to get an IP address from the blocked site. DNS Lists are constantly updated and can be configured to constantly deny any access to any untrusted sites on the DNS list.

Operating System Security

An **active directory** is a database of everything on the network; Computers, user accounts, file shares, printers, groups, and more. This is a primarily windows based system. We can manage all of our authentication from this central resource. We can use them to create access permissions with this as well and assign them to users or groups.

Group policies are security settings made for a group of users or even just an individual user.

Linux traditionally uses DAC(discretionary access control) but a kernel linux(an SElinux) adds MAC(mandatory access control) to the OS.

Secure protocol

Encrypting data is important
Some protocols are not secure like FTP and HTTP
You can verify what is being encrypted by using a packet capture.

Your goal should always be to use a secure protocol, and if that is not an option then it is better to not use that service at all.

Remember port numbers and which are secure and insecure. Their number doesn't always guarantee encryption, always check with the server to make sure it is enabled.

You may want to use a method of encrypting all traffic into the network,like configuring wpa3 instead of open access. Also like using a VPN. may require additional tools and software.

Email Security

It's very easy to spoof an email.
We have had to add on additional security features as time went on to try and mitigate risks with emailing.

A mail **gateway** is a device that gatekeepers all mail into your server. It uses DNS to check if the email is valid. Many times mail gateways are put into a screening zone or DMZ.

SPF protocol(send policy framework) configures allowed emails from a dns txt list.
DKIM(domain key identified mail) digitally signs the transport process and verifies that it is coming from the domain it says it is.

DMARC(domain based message authentication reporting and conformance) allows the system to take all the flagged mail that did not make it through. We can set specific actions in a DNS TXT record to tell what to do with those marked messages. Compliance reports are sent to the administrator.

Monitoring Data

FIM(file integrity monitoring) allows us to know if files have been changed. We put this software on files that are never meant to be changed. On windows we use the **SFC(system file checker)** and on linux we could use **tripwire.**

Many options for HIPS

DLP(see earlier)
-use an endpoint DLP on a client

DLPs allow for USB blocking and prevent USBs from working on a system.

Email DLP looks for outbound/inbound data that may be transferred. Blocks keywords identity imposter and quarantines email messages. Can be configured to block fake wire transfers and financial info.

Endpoint security

Defense in depth is applied here
Edge monitoring means looking at all traffic going in and out of the network
Access control provides control over who has what authorization and who can be authenticated into or around the network.
Posture assessment checks different parameters that can be used to trust a new device into the network. (certificate, mandatory apps, running updated antivirus, etc)

Posture assessment types:
-Persistent agent, is permanently installed and constantly checks health,
-Dissolvable agents, only used when called upon.
-Agentless (NAC), are Integrated with AD(active directory) and only works upon logins/logouts.

If something doesn't pass the **posture assessment** a common mitigation strategy is to quarantine the device.

EDR(endpoint detection and response) see earlier

XDR(extended detection and response) is an evolved EDR. It uses automation of more than one system to interpret and respond to data. Can correlate endpoint, network, and cloud data. Includes behavior analytics.

4.6 Identity and access management

Data can be anywhere and accessed from anywhere without proper configuration.
IAM means to give users access to and manage their ID on a network
Access control in this context means users only get access to what they need.

Starts with the creation of a user account and ends with deactivation.

Provisioning and deprovisioning changes access upon an event, like hiring, firing, promotions, or transfers.
Another big part of IAM is identity proofing. Should be a formal process called **resolution** to verify the Identity of the user.
Requires Additional validation like:
-Something you know
-Somewhere you are
-Something you are
-Something you know

All of it needs to be verified through a process called **attestation** which requires additional verification like in-person meetings and government documents.

Access control

Considered authorization
Least privilege(see above)

Mandatory access control assigns a label to each system and database. Like confidential, top secret and public. The admin decides who gets to use what
Discretionary access control allows the owner of the data complete control over access.
Rolebased access control is based on a job function. Certain groups have group policies which determine what they can do.
Rule based access control is based on rules made by an administrator. Each object has rules that allow or deny access based on if the user meets the criteria defined in the rules.
Attribute based access control is based on many different criteria to determine exactly what type of controls a user can have over an object.

Time of day restrictions limit access during times of day.

Multi Factor authentication

Something you know - password or PIN
Something you have - smart card, a USB security key, hardware/software token devices,sms codes
Something you are - Biometrics
Somewhere you are -login location

Password security

Stop spraying and brute force with complexity(entropy)
Ideally as long as possible and uses three character groups
A **password manager** allows you to store all your passwords in one database.

Passwordless authentication is like FaceID or a windows pin. Commonly alongside a password

Just in time permissions are when you receive limited access for a limited amount of time. Expires after the deed is done.

Central clearing house/password vault will store the temporary credentials and then send them to the Justintime user when needed. But reconfigure the login to make sure it is secure after access is revoked.

4.7 Scripting and automation

Scripting and automation is using code to automatically do a function.

Automation benefits are : saves time, enforces security baselines, creating scripts for creating configurations or duplicate systems with similar configurations, Scaling up a system is far easier with automation inside the cloud, employee retention as it creates automation for the boring repetitive tasks, constant monitoring and alerts with fast reaction time, work force multiplying.

Many orgs automate onboarding and offboarding. An onboarding script can automatically create user accounts.

Guard rails are another automation task that automatically validates all inputted data and makes sure it won't cause a problem
Ticket creation is an automated service

Can routinely automatically audit systems

Script considerations:
-Complexity
-Cost to develop
-Could be a Single point of failure
-Technical debt is when a script is used to hide vulnerabilities, can cause more problems
-Ongoing support, as maintenance is a cost

SSO(single sign on) allows you to log in once and acquire access to all of the resources you need. Usually on a timer and your Authentication protocol needs to work with SSO.

LDAP(lightweight directory access protocol) protocol for accessing large databases and directories on a network**. X.500** was written by the ITU(international telecommunication union) and it is the standardized protocol for this. The legacy version was called DAP and worked on the OSI. Was renamed because of its new efficiency.
X.500 utilizes a directory information tree for its hierarchy.

SAML(security assertion markup language) is an open standard for authentication and authorization. Does Not work with Mobile, so it is somewhat deprecated.

Oauth(open authorization) is more modern and includes mobile devices. It's a framework that uses OpenID to provide authentication and authorization.

Federation is like signing into a third party account using google or facebook.

Interoperability is when some services require other services to provide authorization and authentication.

Variable length Subnet masking(VLSM)- divides one IP into individual subnets with their own masking to see them beyond their parent IP.

4.8 Incident Response

Examples of incidents:
-Ddos
-Malware is installed
-Confidential da is stolen
-A user installs a backdoor

Read the NIST SP 800-61 to understand fully about incident response. Its full spectrum of response protocol

Prepare by having an updated contact list and a Go-bag. A backup system, laptops, removable media, forensic software, and event logs should all be in this go-bag. Another thing that should be available should be a network of resources including baselines and critical files.
Have copies of applications and OS images to easily replace anything that might be malicious or corrupted.

Attacks are always happening so we need to always have easy access to proper policies for response.

Analysis of incidents are used to determine origin and method of attack in order to properly respond.

We need to immediately quarantine any system affected by an attack.

We can test malware by running them on a Sandbox. We do this to compare how an attack might occur on the actual system.

Once an incident is over we need to recover. This could mean, however not limited to, replacing software, patching or changing access controls

A post incident meeting is when everyone gets in a room and discusses how to better respond in the future. It is best to have it as soon as you have recovered.

Train the team in:
-Initial response
-Investigation plans
-Incident reporting
-Recovery plan
-more

Incident planning

Test process,skills and procedures before an actual event. Allows us to know how to change response if need be in a safer environment.

Running a full scale event takes time and money, so we have different types of testing/training to fit the needs of your organization

A tabletop is the smallest and is a tabletop step by step discussion of how to respond to an incident. Everyone is involved in different steps of incident response.

Simulations are like fake helpdesk calls, forced data exfiltration, or phishing tests. We can use them to analyze users breaking AUP or if our monitoring software picks up certain flags.

A root cause analysis is asking “why?”. Helps us create a set of conclusions based on the facts of an incident. We use a step by step look at how an attacker may have entered a system and why. There could be many root causes so look broadly.

Threat hunting is a process of looking for vulnerabilities. It is difficult to do this until an attack actually occurs. We can use an IPS that actively prevents certain vulnerabilities but we also need to stay up to date on any vulnerabilities or systems may have, whether that be on the OS or the hardware itself.

Digital Forensics

The process of collecting data about data about and during a security event. We then can use this data in any legal proceeding. **RFC 3227** is the guidelines for data collection, retention, and archiving best practices. Take notes on all new data gathered

One type of data acquisition request is a legal hold. Sent by an attorney and gives an enumeration of relevant data for a case that must be held onto and stored without tampering. Sent to a data custodian(person who maintains data) and they will decide what gets sent where. All data will be stored in an ESI(electronically stored information) repository. You are responsible to hold onto that data and protect it until its ready to be brought to court.

Chain of custody determines who has access to the data during the legal process. Hashes and digital signatures help us maintain the integrity of data, and these would need to be gathered upon data collection and will be maintained in case a legal hold is ever put onto the data.

Chain of Custody:

1. **Acquisition**. The collecting of the data of any format. Some data may not all be from the same device. A full copy of VM’s is helpful to have. Look for any artifacts, temp files, or recycled files for any leftover data.
2. **Reporting**. Documents the findings of how the data was acquired and stored. A summary of the steps of acquisition and all of the integrity checks put in place, in case of legal proceedings. Provides insight on the security event to explain to anyone who doesn't understand.
3. **Preservation**. Isolating and protecting evidence/data. Creating backups is key. Collecting live data is important in a modern world, so we need to manage how long we need to hold all of our incoming data.
4. **E discovery.** Process of preparing a review of data. About inquiring and reviewing not analyzing.

Log Data

Security log files are found en masse on our systems. We have seen these in our SIEM studies.

Firewall logs contain IP sources that go through each port and what ports have what traffic.NGFW allows us also to see what applications we use.

Application logs, specific to the app. Event viewer on PC or /log on linux.

Endpoint logs. Logon events, policy changes, system events, processes, account management and directory services, etc are all examples of what could be found in an endpoint log. Usually rolled up into the SIEM.

Most OS keep a log file of its own security events. Stuff like authentication, brute force attempts, and file changes are found here. Can also monitor and alert certain events from this log data.

IDS/IPS logs, remember these are usually built into NGFW. Logs contain information on predefined vulnerabilities. Can be correlated with all your other devices on the SIEM.

Network logs are found on your network infrastructure, like switches, routers, access points, and VPN concentrators. They test for any changes in the network, like routing updates, authentication issues, or predefined network issues.

Metadata is data that describes data.

A **packet capture software** allows you to capture detailed information at the packet level. CAn be wired in or OTA(over the air). Wireshark

5.0

5.1 Security policies

These are the rules you follow to provide CIA

An **Information security policy** is a detailed list of every type of incident and event that may happen in an organization. What happens with malware? How do you connect from home? When do you reset your password?

A policy that applies to everyone is an AUP(Acceptable Use Policy) and it enforces how everyone MUST use their devices.

Business continuity is how we function in case of emergencies.(EX: when the POS goes down and you have to write down credit cards.) Plan and test your plan BEFORE it happens.

A **DRP(disaster recovery plan)** is a way to get back to function after a major incident. Should have one for every possible incident.

Security policies should be in effect for any incidents. (EX: DOS and malware or for even confidential information leaks)

CIRT(Computer incident response team) isa team trained specifically for these types of incidents

NIST 800-61 rev 2 is a guide to handling computer security incidents

SDLC(software development lifecycle) has no best way to develop but a framework and plan is recommended to keep everyone on track. **AGILE/RAD** is a faster application development process that is cyclical and tests as you develop it. **Waterfall** is when the development process is linear.

Security Standards

We rely on standards in the industry, which are formal descriptions of processes.
-ISO
-NIST

Password policies are based on what organization decides what is an acceptable password and form of authentication. May define how to access a network or password expiration policies.

Access control is a standard we use to determine who can access what.

Physical security could also be standardized in an organization.

Security Procedures

Change management(see earlier) limits downtime confusion and mistakes.

Onboarding includes adding a new hire or transfer account with their proper account permissions.
Offboarding includes what to do with a user's data and hardware after they leave an organization.

Playbooks define a set of steps to follow how to respond to an event.
Playbooks are put into a **SOAR(security orchestration, automation, and response)** to allow the integrated system to automate step by step processes written in the playbook.

We need to constantly monitor and revise our policies as our industry evolves.

Private Governance starts with a board, who are a panel of specialists or directors, who set broad tasks or requirements to reach a goal. Then a Committee decides how the organization decides will go about completing the task.They then present it to the board for approval.

Governmental policies are concerned with politics and the law. Mostly everything is discussed publicly and revolves around keeping classified info classified and secure. Much higher standards.

Security Considerations

Regulations are commonly mandated by the industry you are working in. Always familiarize yourself with the regulations. **SOX(sarbanes Oxley act)** focuses on the finances of an organization.it is very common. This means we should always ensure the CIA has financial info. **HIPPA** protects health information

Its team is responsible for data during a legal hold.

Organizations are legally mandated to disclose data breaches in a reasonable timeframe. Determined by local laws and industry regulations.

Data Roles and Responsibilities

Data owner is a higher level person in an organization. They are responsible for a broad scope of data in their specialty.

Data controller manages how the data will be used

Data processor uses the data

Data custodian is responsible for the data's security. Ensures confidentiality and integrity. May be assigned to making sensitivity levels for each piece of data. Often implements access control as well.

5.2 Risk Management

As an organization grows so does risk.
internal/external risk
Every organization does risk assessment different.
- One time risk assessment is an assessment for a one time event. Like an analysis of absorbing a business or a new software rollout.
-Ad hoc assessment is performed for one specific purpose. Like if your CEO discovers a risk similar companies have and then we would look at how that specific threat will affect us.
-Recurring assessments are done over standard intervals to keep up with any new risks that may come up. The PCI DSS enforces a once a year assessment over your payment card security risks.

Risk analysis

Determining levels of risk can vary based on the amount individuals factors are associated with said risk.

A qualitative is looking at the qualities of a risk.
Quantities are stats and values that represent a risk.

-**ARO(annualized rate of Occurrence)**
-**AV(Asset Value)** how much an asset means(in $s) to a company based on use and need.
-**EF(exposure factor)** is a percentage of value of an asset that is lost due to an incident.

SLE(single loss expectancy)=AV x EF

ALE(annualized loss expectancy)= ARO x SLE

Life is the most important thing to protect.

Likelihood is qualitative and probability is quantitative

Risk Appetite Posture is a qualitative description for readiness to take on risk

Risk tolerance is how much risk you are willing to take for a desired outcome.

A **risk register** is a document that describes each risk and indicates what they are and mitigation strategies for each.

A **risk owner** manages the risk

A **Risk threshold** needs to be balanced between cost of mitigation and what the risk could cost the company.

Risk Management

Acceptance
Transference
Mitigation
Avoidance

Business impact analysis

Recovery time objective(RTO) is what most operators want to know. It's how long (in time units) it is going to be before the organization is up and running.
Recovery Point Objective(RPO) is the actions that are done that indicate recovery has been completed.

MTTR(mean time to repair) is how fast you can repair equipment

MTBF(mean time between failure) shows how long is between outages on a system. Used in deciding whether to adopt a new device or software.(Total uptime/number of breakdowns)

5.3 Third party risk

Put risk assessment info into your contract with all third parties.

PenTesting is a common form of risk assessment that can be done by or for Third Parties.

Agreement Types

SLA(service level agreement) are the minimum terms for services provided. Includes stuff like uptime and response time. A contract with an **ISP(internet service provider)** is a common SLA.

MOU(memorandum of understanding) are broad goals that two organizations discuss between each other. Very informal and nonbinding.

MOA(memorandum of Agreement) a more detailed MOU, may contain legally binding information but is not a contract.

MSA(master service agreement) outlines all services and exchanges that two parties will follow during an ongoing relationship. A legal contract that sets terms, and sets up a framework for future transactions.

Work order(WO)/Statement of Work(SOW) has a job location and a list of what's expected during a service. Built off the framework of the MSA.

A **NDA(Non Disclosure Agreement)** is a formal contract that prevents anyone outside of the agreement from learning about the information. Unilateral is one way and bilateral is a two way NDA.

Business Partner Agreement(BPA) determines who does what in a partnership. Also documents what to do incase of emergencies and incidents.

5.4 Compliance

The process of following standards, laws, policies, and regulations.
Remember about penalties for breaking compliance on any of these types.
CCO(central compliance officer) manages internal compliance.

Privacy

Remember privacy laws
GDPR
HIPAA